AO 106 (Rev. 04/10) Application for a Search Warrant

USAO# 2018R00157

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

Hotmail Account: advent@hotmail.co.jp controlled by Microsoft Corporation, located at One Microsoft Way, Redmond, WA 98052

Case No. MJ18-369

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, attached hereto and incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1028(a)(7); 1028A; 1029(a)(2)	Identity Theft; Aggravated Identity Theft; Access Device Fraud
18 U.S.C. §§ 1030(a)(4); 1343	Computer Fraud; Wire Fraud
18 U.S.C. § 1956	Money Laundering

The application is based on these facts:

See Affidavit of Special Agent Joel Martini, attached hereto and incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

JOEL MARTINI Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/15/2018

Judge's signature

City and state: Seattle, Washington

James P. Donohue, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Joel Martini, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed for approximately 1 year. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other Cybercrimes. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, Cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training in the acquisition and analysis of digital evidence (both network and host based), responding to computer intrusions and other incidents. I currently hold a Bachelor of Science in Information Systems from Corban University.

2. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately 5 years. As part of that employment, I became familiar with the design and operations of various electronic devices, networks, and websites, including technology described herein.

3. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by an electronic communications service and remote computer service provider, namely, Microsoft Corporation ("Microsoft"), located at Redmond, Washington (generally, "SUBJECT ACCOUNT"). The information to be searched is described in the following paragraphs and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

in Attachment A, which are incorporated herein. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B, pertaining to the following account or user identifier, identified in Attachment A:

advent@hotmail.co.jp ("SUBJECT ACCOUNT #9")

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. This warrant is requested in connection with an on-going investigation in this district by the Seattle Field Office of the Federal Bureau of Investigation (FBI).

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(4) (Computer Fraud); 1343 (Wire Fraud); and 1956 (Money Laundering) have been committed by an individual known as "Matthew Ho," as described below, as well as perhaps other unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes, as described in Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **IP Address**: An Internet Protocol address (or simply "IP address") is a unique numeric address used by devices, such as computers, on the Internet. Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

b. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. **Cloud Computing**: Cloud Computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

d. **Cryptocurrency**: Cryptocurrency is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. Decentralized cryptocurrencies such as Bitcoin now provide an outlet for personal wealth that is beyond restriction and confiscation.

e. **Cryptocurrency Mining**: Cryptocurrency mining is the process by which transactions are verified and added to the public ledger, known as the block chain, and also the means through which new Bitcoin are released.

SUMMARY OF PROBABLE CAUSE

A. Overview

7. The FBI is conducting an investigation into a suspected fraud scheme, believed to have been conducted by and through one or more foreign actors. As discussed below, the FBI received information from multiple U.S. companies regarding the theft and misuse of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

services through the unauthorized use of another person's identity and stolen credit card. The primary suspect, identified as "Matthew Ho" (and hereafter referred to as such), is believed to be a resident of Singapore and the user of **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**, as well as multiple other accounts, some of which are described herein.

8. More specifically, in about October 2017, one or more suspects impersonated and used without authorization personal information of a real person residing in the state of California, Marc Merrill, including his name, address, and credit card information, along with a seemingly authentic email account, namely, mnmerrill25@gmail.com (ACCOUNT #1), to open accounts at multiple online service providers, such as Google and Amazon. Merrill is the co-founder and current co-chairman of Riot Games, a video game developer and eSports tournament organizer based in Los Angeles, California.

9. Thereafter, according to the providers, Ho used fraudulently created cloud services accounts primarily, if not exclusively, as part of a large-scale cryptocurrency mining operation,[1] and in doing so accrued multiple millions of dollars in unpaid cloud service fees and charges. Some of the past due balances were charged to Merrill's credit card, some of which the accountholder paid before the fraud and compromise of the credit card account were discovered.

B. Summary of Investigation

10. In February 2018, Amazon Web Services (AWS), Amazon's cloud services subsidiary,[2] contacted the FBI Seattle Office regarding suspected fraud. According to information provided by AWS, on about January 22, 2018, AWS closed a particular cloud

---

[1] Based on my training and experience and that of other experienced investigators, I know that cryptocurrency mining potentially can prove lucrative particularly given the recent escalation in popularity, and value, of various cryptocurrencies, such as Bitcoin and Ethereum. I also know that current mining practices typically require a large amount of processing power and data usage. In fact, some miners pool resources, sharing their processing power over a network to split the reward.

[2] Amazon is an electronic commerce and cloud computing company based in Seattle, Washington, within the Western District of Washington. Amazon Web Services (AWS) is a subsidiary of Amazon.com that provides on-demand cloud computing platforms to individuals, companies and governments, on a paid subscription basis.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

computing account ("MERRILL ACCOUNT") after identifying several strong indications of fraud. The MERRILL ACCOUNT was opened on about November 2, 2017, under a fraudulent association to an existing, legitimate corporate AWS customer, Riot Games, through use of Merrill's identity and credit card and a fraudulent email account meant to appear legitimate, specifically, mnmerrill25@gmail.com (ACCOUNT #1).

11. According to AWS, through social engineering and the use of Merrill's identity and credit card information, the suspect was able to gain access to substantially elevated levels of cloud computer services. As explained by AWS to investigators,

> Mr. Merrill is the co-founder and President of Riot Games, a video game developer, eSports tournament organizer and publisher. While Riot Games is an AWS customer, the fraudulent account was not a compromise of the Riot Games corporate AWS account. The fraudster used sophisticated social engineering techniques, relying on Mr. Merrill's relationship with AWS and his high net worth to convince AWS employees that this account was legitimate. Additionally, a payment of $135,860.99 was made on 12/03/2017 using the American Express card registered on the account. It is not known if this card was stolen or compromised, but it had been previously used on other accounts associated with Riot Games. The large payment combined with several convincing "customer" contacts allowed this sophisticated fraudster to go undetected for two months.

As noted above, according to AWS, the impersonation of Merrill specifically and AWS's existing cloud service customer relationship with Merrill's company, coupled with a sizeable initial payment charged to Merrill's credit card, American Express ("Amex") ending in -93007, deceived AWS into granting Ho access to an elevated level of cloud computing resources and data usage.

12. According to AWS's initial estimates conveyed to investigators, the fraudulent AWS MERRILL ACCOUNT accrued a balance of roughly $5 million in commercial cloud computing services. AWS conveyed its belief that the MERRILL ACCOUNT was used for cryptocurrency mining based on the data usage volume and patterns.

13. AWS provided investigators with several identifiers and IP addresses and a copy of what was determined to be a fake California driver license bearing Merrill's name

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

provided as verification to open the MERRILL ACCOUNT. AWS further provided the name "Matthew Ho" as a suspect based on its preliminary internal investigation.

14. As part of this investigation, I have reviewed account records for Merrill's Amex account, ending in -93007, which was used to register the fraudulent AWS MERRILL ACCOUNT, described above. The account belongs to Merrill and presumably his spouse. On December 3, 2017, there is a charge to AWS in the amount of $135,861.12:

12/03/17	Amazon Web Services WEB SERVICES	AWS.Amazon.com	WA	$135,861.12

On or about December 20, 2017, the Merrills paid the outstanding balance, or thereabouts, on the Amex account, which included the unauthorized charge to AWS. This charge was later reversed after a fraud report.

15. In February 2018, Merrill's company, Riot Games, also contacted the FBI to advise that Google had reported similar fraudulent activity involving the use of stolen victim information to open a Google Cloud Services account and obtain and pay for cloud services, believed to be used for cryptocurrency mining. Like with AWS, the fraudulent Google account (#01450E-B5EE32-315DF9) (CLOUD ACCOUNT #1) was opened using the name Marc Merrill, his Amex credit card, ending in -93007, and the same fake email account, mnmerrill25@gmail.com (ACCOUNT #1). It was then utilized to also fraudulently purchase Google Cloud computing resources using a stolen or compromised credit card in order to mine cryptocurrency. Further, the Santa Monica, CA address provided for the account appears to be a property actually owned by Merrill.

16. According to information provided by Google, Merrill's Amex card was authorized on November 4, 2017, and thereafter used for 16 payments for cloud computing services through February 22, 2018. Google charged a total of approximately $240,000, or thereabouts, to Merrill's Amex card for this fraudulent cloud services account, but nearly all of that amount was either later reversed/charged back or declined by the issuing bank.

17. Account statements for Merrill's Amex card show numerous sizeable transactions with Google for what appear to be cloud services. For example,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Credits				Amount
11/04/17	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$280.00
11/08/17	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$100.00
11/11/17	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$1,000.00
12/06/17	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$10,000.00
01/05/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$9,775.07
02/04/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$3,362.36
02/15/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$10,000.00
02/17/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$10,000.00
02/19/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$10,000.00
02/20/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$10,000.00
02/20/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$30,000.00
02/21/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$20,000.00
02/21/18	MARC MERRILL	GOOGLE *CLOUD_01450CC@GOOGLE.COM	CA	-$20,000.00

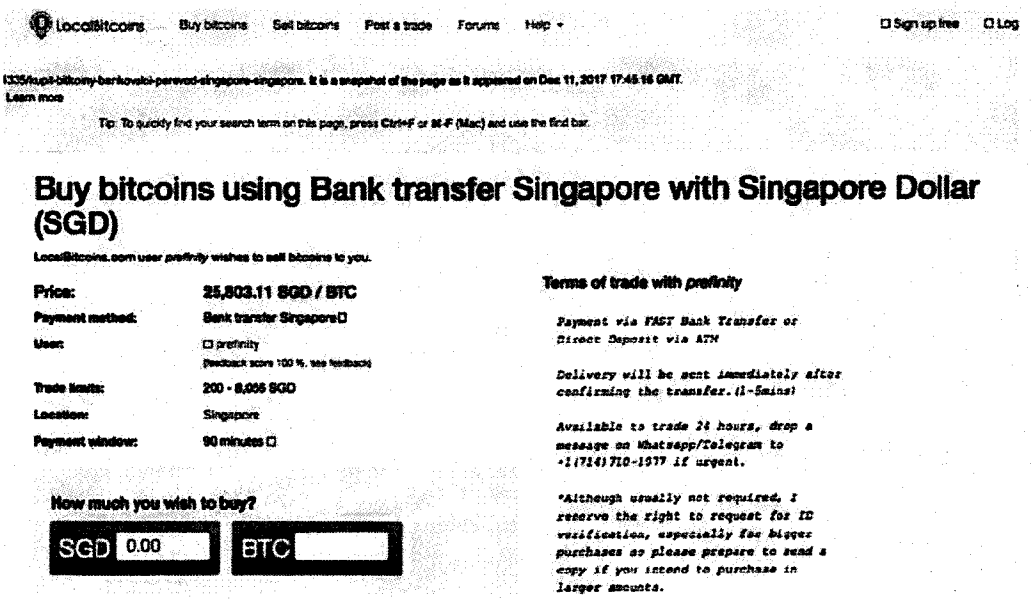
18. According to records provided by Google, mnmerrill25@gmail.com (ACCOUNT #1) was created from a Singapore IP Address (27.125.180.127) on October 19, 2017.

19. Based on its independent inquiry, Google identified the suspect and actual user of mnmerrill25@gmail.com (ACCOUNT #1) as Matthew Ho, age 28 (DOB xx/xx/1990), of 8 Lentor Place, Singapore. Google further provided various additional linked accounts and identifiers it associated with Ho, including Microsoft accounts **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** and prefinity@outlook.jp (ACCOUNT #10), among others, as well as pertinent records, which investigators have reviewed.

20. According to Google, the recovery phone number for the fake Merrill email account mnmerrill25@gmail.com (ACCOUNT #1) also appears in association with an individual using the alias "prefinity" selling Bitcoin in Singapore on a cryptocurrency website: localbitcoins.com.[3]

[3] Google initially identified the cryptocurrency website as localbitcoins.net. Upon further review, it appears that the correct website is localbitcoins.com.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



LocalBitcoins Buy bitcoins Sell bitcoins Post a trade Forums Help ▾ Sign up free Log

...335/rupt-bitkony-berkowski-perwad-singapore-singapore. It is a snapshot of the page as it appeared on Dec 11, 2017 17:45:16 GMT.
Learn more

Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar.

Buy bitcoins using Bank transfer Singapore with Singapore Dollar (SGD)

LocalBitcoins.com user *prefinity* wishes to sell bitcoins to you.

Price:	25,803.11 SGD / BTC
Payment method:	Bank transfer Singapore
User:	prefinity (feedback score 100 %, see feedback)
Trade limits:	200 - 8,005 SGD
Location:	Singapore
Payment window:	90 minutes

How much you wish to buy?

SGD 0.00 BTC

Terms of trade with *prefinity*

Payment via FAST Bank Transfer or Direct Deposit via ATM

Delivery will be sent immediately after confirming the transfer. (1-5mins)

Available to trade 24 hours, drop a message on Whatsapp/Telegram to +1(714)710-1577 if urgent.

Although usually not required, I reserve the right to request for ID verification, especially for bigger purchases so please prepare to send a copy if you intend to purchase in larger amounts.

21. Based on usage records (cookie overlap), Google identified several Google email accounts and YouTube accounts that appear linked to the actual user of mnmerrill25@gmail.com (ACCOUNT #1), including surrenderous@gmail.com (ACCOUNT #2), matt@prefinity.com (ACCOUNT #3), faeianef@gmail.com (ACCOUNT #4), xenatic@gmail.com (ACCOUNT #5), snzqdoggy@gmail.com (ACCOUNT #6), and marcgashmore@gmail.com (ACCOUNT #7). According to Google, it is the service provider for this prefinity.com account.

22. According to Google, the name on account faeianef@gmail.com (ACCOUNT #4) is "Faeia," and formerly included a Singapore recovery phone number. The recovery email address for the account is prefinity@outlook.jp (ACCOUNT #10). Notably, the username "prefinity" reoccurs as the Bitcoin vendor on localbitcoins.com as well as in relation to a Google email address also believed to be used by Ho, matt@prefinity.com (ACCOUNT #3), described below.

23. According to Google records, the name on account surrenderous@gmail.com (ACCOUNT #2) is Matthew Ho (DOB xx/xx/1990). The account has a Singapore recovery phone number and a recovery email address of **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**, which, as discussed below, appears in relation to various other accounts

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

associated with Ho. Further, the name and address provided for the associated Google Payments account is Ho Jun Jia, 8 Lentor Place, Singapore 788995.

24. According to Google records, the same Singapore IP Address (27.125.180.127) used to create mnmerrill25@gmail.com (ACCOUNT #1) was also used to access surrenderous@gmail.com (ACCOUNT #2) in August 2017. Moreover, the two accounts share multiple login IP Addresses, which suggest that the same user is accessing both accounts. Set forth below are some examples from Google records:

a. On November 27, 2017, at 03:10:37-UTC, a particular IP Address (104.238.46.241) was used to log into the account surrenderous@gmail.com (ACCOUNT #2). Approximately 15 minutes later, at 03:26:42-UTC, and on multiple other occasions the same day, mnmerrill25@gmail.com (ACCOUNT #1) was accessed from that same IP address (104.238.46.241).

b. On November 29, 2017, mnmerrill25@gmail.com (ACCOUNT #1) was accessed approximately five times from an IP Address (119.74.28.26) that also was used to log onto surrenderous@gmail.com (ACCOUNT #2) several days prior and on multiple occasions in January 2018.

c. The final log on of mnmerrill25@gmail.com (ACCOUNT #1) appearing on the Google records occurred on May 7, 2018, at 07:26:26-UTC, from a particular IP Address (42.60.69.244). That same IP Address was used to access surrenderous@gmail.com (ACCOUNT #2) on numerous occasions throughout April and May 2018, which includes multiple instances on May 7, 2018, including at 06:51:22 and a failed log in attempt at 06:55:53-UTC.

There are other examples of IP Address overlaps observed in the records.

25. According to Google records, the name on account matt@prefinity.com (ACCOUNT #3) also is Matthew Ho (DOB xx/xx/1990). The account has a Singapore recovery phone number[4] and a recovery email address of **advent@hotmail.co.jp**

[4] The recovery phone number is a different Singapore phone number than associated with surrenderous@gmail.com (ACCOUNT #2).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(SUBJECT ACCOUNT #9), the same as associated with surrenderous@gmail.com (ACCOUNT #2). The name and address on the associated Google Payments account is Matthew Ho, 8 LENTOR PL, Singapore 788995, and has a registered Mastercard debit card issued in Singapore with cardholder name "Matthew Ho." The user of matt@prefinity.com (ACCOUNT #3) also has a YouTube account, under the name "Matthew Ho" (DOB xx/xx/1990). According to Google, a cloud account (#005FC3-CD09EC-426975) ("CLOUD ACCOUNT #2") is associated with matt@prefinity.com (ACCOUNT #3) and user Matthew Ho.

26. According to records provided by Google, matt@prefinity.com (ACCOUNT #3) also shares multiple login IP Addresses with both mnmerrill25@gmail.com (ACCOUNT #1) and surrenderous@gmail.com (ACCOUNT #2). For instance, the IP Address (104.238.46.241) used to access surrenderous@gmail.com (ACCOUNT #2) and mnmerrill25@gmail.com (ACCOUNT #1) on November 27, 2017, was also used to access matt@prefinity.com (ACCOUNT #3) on the same date. Account logs for matt@prefinity.com (ACCOUNT #3) also reflect usage of IP address (119.74.28.26), which as discussed above was used to access surrenderous@gmail.com (ACCOUNT #2) and mnmerrill25@gmail.com (ACCOUNT #1).

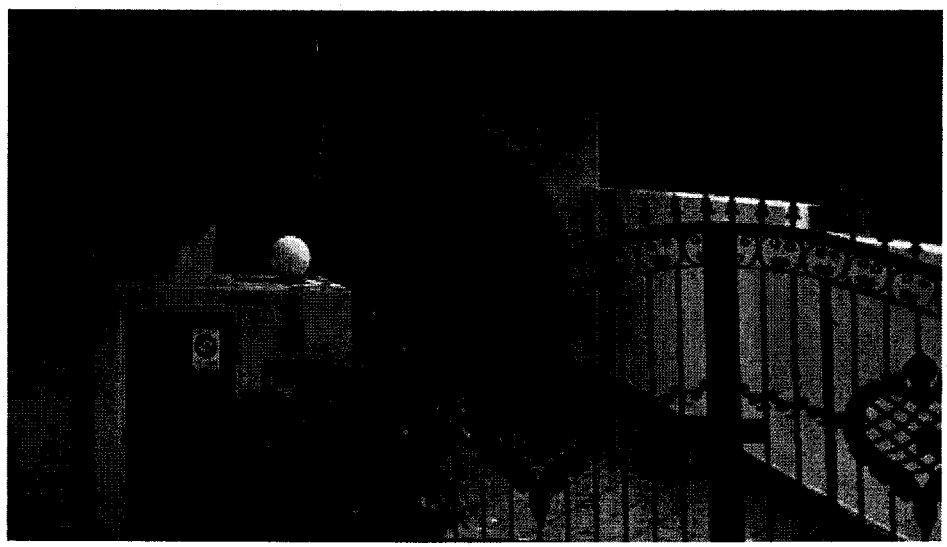
27. According to Google, email address **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**, the common recovery email account for both ACCOUNTS #2 and #3,[5] is linked to a particular Facebook profile, Facebook User ID 1224618568 (FACEBOOK ACCOUNT #1).

28. As part of the investigation, investigators have viewed the public aspects of FACEBOOK ACCOUNT #1. The name on the Facebook account is Matthew Ho. A prominent profile image on FACEBOOK ACCOUNT #1 shows various Mazda RX-7s.

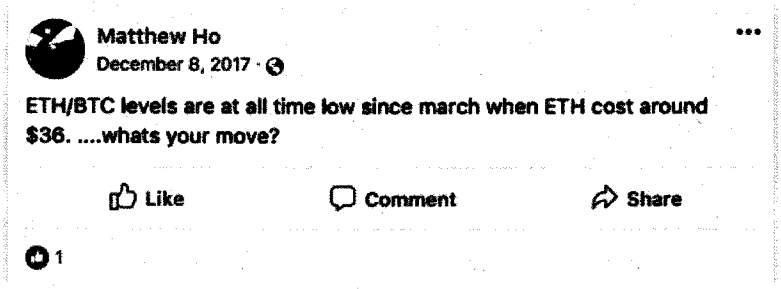
[5] The subscriber records for mnmerrill25@gmail.com (ACCOUNT #1) do not contain a recovery email address for the fake account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Investigators have also conducted inquiries regarding Ho's suspected address, 8 Lentor Place, Singapore. Notably, what appears to be a Mazda RX-7 is visibly parked in the driveway of that residence on Google Maps street view:



29. From his posts on FACEBOOK ACCOUNT #1, Matthew Ho also indicates interest in cryptocurrency. For instance, on about December 8, 2017, Ho posted about the current price of Bitcoin (BTC) and Ethereum (ETH):



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

It is noteworthy that the criminal activity and suspected cryptocurrency mining that is the subject of this investigation was ongoing in December 2017 at the time of this post. It is further noteworthy that Ho asks others "whats your move?" while he also, it appears, actively sells cryptocurrency.

30. According to records obtained from Facebook, FACEBOOK ACCOUNT #1 is registered to Matthew Ho, with vanity name "inksandneedles" and registered email addresses **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** and inksandneedles@facebook.com. The account was created in January 2009. Moreover, various credit cards in the name of Matthew Ho are registered to FACEBOOK ACCOUNT #1,[6] as is a PayPal account further linked to ciel@projectquintessance.com (ACCOUNT #8), discussed further below.

31. According to records obtained from Facebook, FACEBOOK ACCOUNT #1 similarly shares multiple common login IP Addresses with mnmerrill25@gmail.com (ACCOUNT #1) and other online accounts known to be used by Ho, including 119.74.28.26 and 42.60.69.244, discussed above. In fact, according to Facebook records, the Singapore IP Address (27.125.180.127) used to create the fraudulent account, mnmerrill25@gmail.com (ACCOUNT #1), was also used to access FACEBOOK ACCOUNT #1 leading into October 2017, as illustrated below:

IP Address 27.125.180.127
Time 2017-10-12 15:01:49 UTC
Action Login

. . .

[6] There is also a credit card in another name registered to the Facebook account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

IP Address 27.125.180.127
Time 2017-09-01 04:17:33 UTC
Action Login

IP Address 27.125.180.127
Time 2017-08-30 07:29:32 UTC
Action Photo uploaded

IP Address 27.125.180.127
Time 2017-08-27 08:10:59 UTC
Action Photo uploaded

IP Address 27.125.180.127
Time 2017-08-27 07:30:26 UTC
Action Photo uploaded

IP Address 27.125.180.127
Time 2017-08-20 05:35:59 UTC
Action Login

By way of further example, according to record logs, on May 7, 2018 (UTC), both mnmerrill25@gmail.com (ACCOUNT #1) and FACEBOOK ACCOUNT #1 were accessed using IP address 42.60.69.244 --- *i.e.*, mnmerrill25@gmail.com (ACCOUNT #1) at approximately 7:26 a.m. UTC:

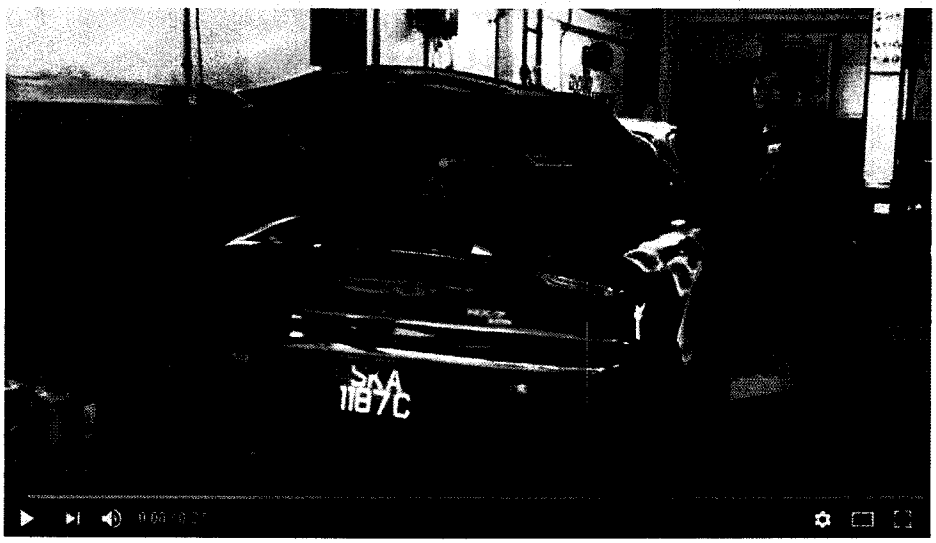
Time	IP Address	Type
2018/05/07-07:26:26-UTC	42.60.69.244	Login

and FACEBOOK ACCOUNT #1 at approximately 8:01 a.m. UTC, as well as on multiple dates thereafter:

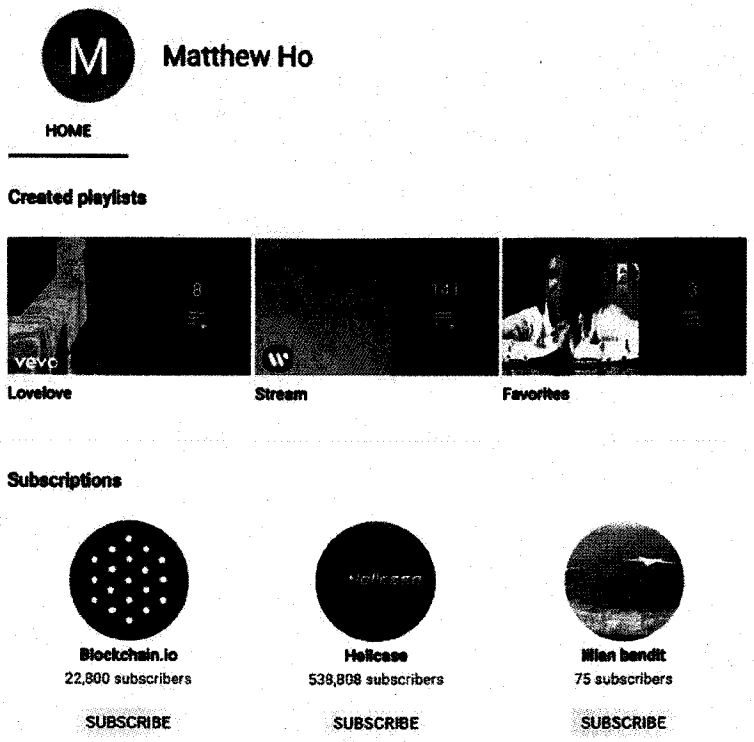
IP Address 42.60.69.244
Time 2018-05-07 08:01:31 UTC
Action Login

32. According to Google records, email address **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** is also the recovery email address for Google account ciel@projectquintessance.com (ACCOUNT #8). The name on the account also is Matthew Ho, and has the same recovery phone number as surrenderous@gmail.com (ACCOUNT #2). The user of ciel@projectquintessance.com (ACCOUNT #8) also maintains a YouTube account, which has posted a video of a Mazda RX-7 that appears similar to the vehicle, if not the same vehicle, parked at 8 Lentor Place, Singapore on Google Maps.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



Additionally, the above referenced YouTube account bears the name Matthew Ho and shows at least one subscription to what appears to be cryptocurrency videos (Blockchain.io).



33. In July 2018, Microsoft provided records relating to **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** and prefinity@outlook.jp (ACCOUNT #10), which included limited information regarding e-mail, OneDrive, Skype, Xbox, and payment accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Microsoft further advised that prefinity@outlook.jp (ACCOUNT #10) is an alias name for **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**. Specifically, according to the Microsoft return: "You have requested account prefinity@outlook.jp. Account prefinity@outlook.jp is an ALIAS of account advent@hotmail.co.jp; as such, we are providing the requested data for account advent@hotmail.co.jp." Investigators interpret this to mean that, because the two accounts are effectively one and the same, Microsoft only produced records for **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**.

34. According to records obtained from Microsoft, the registration information for **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** appears to reflect a registrant located in Japan:

Signin Name	First Name	Last Name	Region / State	Postal Code	Country	Time Zone
advent@hotmail.co.jp	れいな	宮咲	Tokyo-to	571-8501	Japan	Tokyo, Japan - JST

However, the payment profile records associated with **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** includes Matthew Ho of 8 Lentor Place, Singapore, and bears the ID: 83d44bcd-de56-464b-bc19-f586c50421a4:

Commerce Payment Instrument Records

Query For: advent@hotmail.co.jp
Query Type: AccountName

Profiles

First Name	Last Name	Microsoft Account	Billing Email	Type	Id
Matthew	Ho	advent@hotmail.co.jp	advent@hotmail.co.jp	consumer	83d44bcd-de56-464b-bc19-f586c50421a4
Matthew	Ho	advent@hotmail.co.jp	advent@hotmail.co.jp	Classic	-UFaIQAAAAABAACg
Matthew	Ho	advent@hotmail.co.jp	matt@prefinity.com	Classic	qUPe2wAAAAABAACg
Carolyn	Migliori	advent@hotmail.co.jp	noelamores@corestratos.com	Classic	osTlggEAAAABAACg

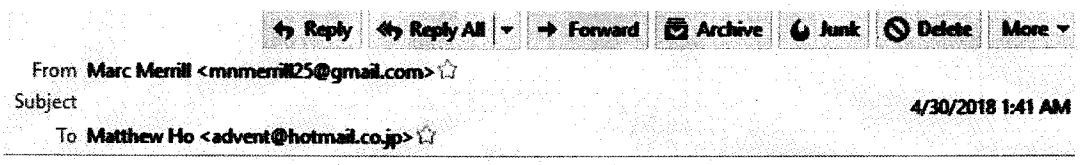
Addresses

Address	Telephone	Id
8 Lentor Place , Singapore, , SG 788995		83d44bcd-de56-464b-bc19-f586c50421a4
950 Muschlitz Road , Nazareth, PA, US 18064		59a097db-b131-5589-08fa-09ddcfe82a09
950 Muschlitz Road , Nazareth, PA, US 18064		87ef3f0e-2a77-54ed-9196-bb6d21098f17

The records also identify matt@prefinity.com (ACCOUNT #3) as an alternative billing email to **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

35. The records obtained from Microsoft also included e-mail identifiers and header information (no content). This information revealed at least one communication sent between mnmerrill25@gmail.com (ACCOUNT #1) and **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**:



Notably, the username of **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** is Matthew Ho.

36. Additionally, the e-mail identifiers and header information included references to cryptocurrency. For instance, more specifically, the email headers for **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** indicate extensive communication with various cryptocurrency entities worldwide, including localbitcoins.com where, as discussed above, it is believed the target of this investigation marketed and sold cryptocurrency under the alias name "prefinity."

Correspondents	Date
← no-reply@localbitcoins.com	7/14/2017 8:26 AM
← no-reply@localbitcoins.com	7/23/2017 2:13 PM
← no-reply@localbitcoins.com	7/30/2017 1:33 AM
← no-reply@localbitcoins.com	7/30/2017 12:30 PM
← no-reply@localbitcoins.com	8/1/2017 7:20 AM
← no-reply@localbitcoins.com	8/1/2017 7:25 AM
← no-reply@localbitcoins.com	8/1/2017 6:51 PM
← no-reply@localbitcoins.com	8/4/2017 12:07 PM
← no-reply@localbitcoins.com	8/4/2017 12:34 PM
← no-reply@localbitcoins.com	8/4/2017 1:23 PM
← no-reply@localbitcoins.com	8/4/2017 1:26 PM
← no-reply@localbitcoins.com	8/4/2017 1:46 PM
← no-reply@localbitcoins.com	8/4/2017 1:47 PM
← no-reply@localbitcoins.com	8/6/2017 2:52 PM
← no-reply@localbitcoins.com	8/8/2017 10:04 AM
← no-reply@localbitcoins.com	8/8/2017 10:26 AM
← no-reply@localbitcoins.com	8/8/2017 10:27 AM

37. The records obtained from Microsoft further show that **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** regularly communicated with Google Cloud Services around

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the timeframe of the fraudulent Google Cloud Services purchases previously provided by American Express, discussed above.

Correspondents	Date
← Google Cloud	4/10/2017 7:14 PM
← Google Cloud	4/17/2017 6:53 PM
← Google Cloud	4/24/2017 7:38 PM
← Google Cloud	8/14/2017 6:05 PM
← Google Cloud	8/28/2017 6:04 PM
← Google Cloud	9/5/2017 6:09 PM
← Google Cloud	9/20/2017 6:23 PM
← Google Cloud	9/26/2017 6:49 PM
← Google Cloud	11/16/2017 7:02 PM
← Google Cloud	12/4/2017 6:52 PM
← Google Cloud	2/11/2018 5:17 PM
← Google Cloud	2/27/2018 6:28 PM
← Google Cloud	3/6/2018 9:57 PM
← Google Cloud	3/12/2018 6:06 PM
← Google Cloud	3/14/2018 6:53 PM
← Google Cloud	3/26/2018 6:07 PM

Based on my training and experience, and my involvement in this investigation, I believe that the contents of these and other communications include evidence of the criminal activity under investigation, and that various accounts described herein served as instrumentalities of the crime.

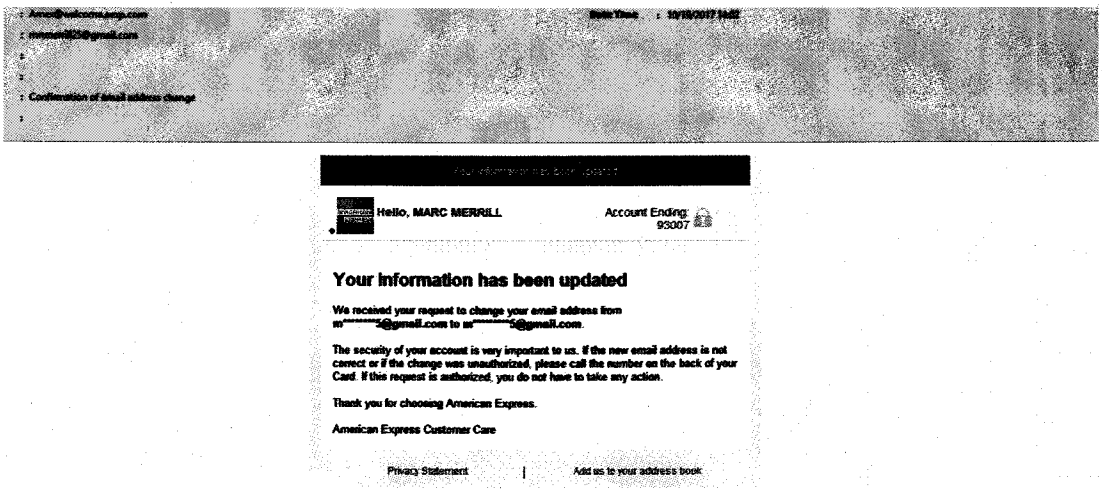
38. The IP connection logs for the account further link **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** to Matthew Ho and the fraudulent activity under investigation. For example, as discussed above, the final known log on of the fraudulent Google account mnmerrill25@gmail.com (ACCOUNT #1) according to records obtained to date occurred on May 7, 2018, from a particular IP Address (42.60.69.244). According to IP connection logs provided by Microsoft, between May 21, 2018 and June 11, 2018 (the date range provided), that same IP Address (42.60.69.244) was used to log into **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)** on more than 50 occasions.

39. On about June 14, 2018, the Honorable Brian A. Tsuchida authorized search warrants for various accounts maintained by Google, namely, mnmerrill25@gmail.com (ACCOUNT #1), surrenderous@gmail.com (ACCOUNT #2), matt@prefinity.com (ACCOUNT #3), CLOUD ACCOUNT #1 and CLOUD ACCOUNT #2, discussed above.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Investigators recently received a partial production of responsive material from Google, which is in the process of being reviewed, and await additional material that are forthcoming.

40. Preliminary review of the partial production of Google records revealed communications and evidence related to the criminal activity under investigation. For instance, mnmerrill25@gmail.com (ACCOUNT #1) contained a message confirming that the e-mail address for Merrill's Amex account, ending in -93007, had been changed to mnmerrill25@gmail.com (ACCOUNT #1):



Hello, MARC MERRILL

Account Ending: 93007

Your information has been updated

We received your request to change your email address from m*******5@gmail.com to m*******5@gmail.com.

The security of your account is very important to us. If the new email address is not correct or if the change was unauthorized, please call the number on the back of your Card. If this request is authorized, you do not have to take any action.

Thank you for choosing American Express.

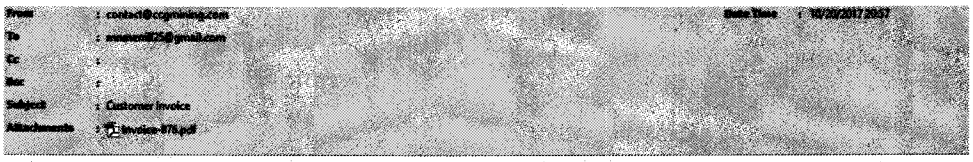
American Express Customer Care

Privacy Statement | Add us to your address book

Notably, this account information change occurred on October 19, 2017, immediately after (and possibly the same day) mnmerrill25@gmail.com (ACCOUNT #1) was created.

41. Additionally, emails show that, within days of creating the fake account, the user of mnmerrill25@gmail.com (ACCOUNT #1) used the account to impersonate Merrill, to generated accounts in his name, and to attempt to access his accounts. For instance, the suspect (Ho) appears to have used Merrill's identity to create obtain cryptocurrency mining-related services. On about October 20, 2017, mnmerrill25@gmail.com (ACCOUNT #1) received an email address to "Marc Merrill" from a contact@ccgmining.com, which appears to convey an invoice:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



CCG

Dear Marc Merrill,

This is a notice that an invoice has been generated on Friday, October 20th, 2017.

Your payment method is: PayPal

Invoice #876
Amount Due: $29.49USD
Due Date: Friday, October 20th, 2017

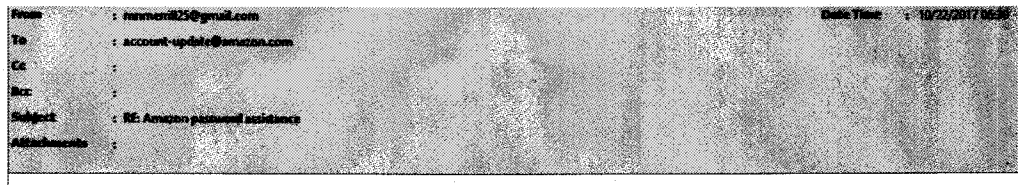
Invoice Items

BITCOIN 200 GH/s $29.49USD
Your Bitcoin Wallet: 1CmvcgaxzyFaWg1rvY2MBX1qxZx8oNWKBL

Sub Total: $29.49USD
Credit: $0.00USD
Total: $29.49USD

You can login to your client area to view and pay the invoice at
https://ccgmining.com/viewinvoice.php?id=876

According to the company's website (www.ccgmining.com), CCG Mining provides information and services related to cryptocurrency and mining and markets itself as "an international company offering comprehensive solutions based on blockchain technology." On October 22, 2017, the suspect sent an email from mnmerrill25@gmail.com (ACCOUNT #1) that appears to be an attempt to gain access to Merrill's Amazon accounts, which, based on my training and experience, I know likely would contain additional personal and financial information:



Hi,

I am unable to log in, it tells me password is incorrect even after changing it. Kindly Assist.

Sent from Mail for Windows 10

42. On about July 3, 2018, the Honorable Mary Alice Theiler authorized a search warrant for Facebook User ID 1224618568 (FACEBOOK ACCOUNT #1), discussed above.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Investigators received and are in the process of examining responsive material from Facebook.

43. Similar to the records provided by Google, a preliminary review of Facebook's return identified evidence linking the user of FACEBOOK ACCOUNT #1 (Matthew Ho) to the criminal activity under investigation. For instance, FACEBOOK ACCOUNT #1 contained conversations that appear to discuss cryptocurrency, account numbers, and the need for credit cards with matching IDs.

Author Matthew Ho (1224618568)
Sent 2017-12-05 06:53:14 UTC
Body If you have the acc numbers

Author Matthew Ho (1224618568)
Sent 2017-12-05 06:53:09 UTC
Body But not an issue i can sell ethereum and deposit directly

Author Matthew Ho (1224618568)
Sent 2017-12-05 06:52:50 UTC
Body PREFERABLY 35

Author Aaron Chia (741926884)
Sent 2017-12-05 06:52:33 UTC
Body need to have one dollar inside nia right

Author Aaron Chia (741926884)
Sent 2017-12-05 06:52:21 UTC
Body easy to get also.

Author Matthew Ho (1224618568)
Sent 2017-12-05 06:52:00 UTC
Body I need debit or credit cards matching those ids

Author Aaron Chia (741926884)
Sent 2017-12-05 06:52:00 UTC
Body you need device spoofing all i can do

Author Aaron Chia (741926884)
Sent 2017-12-05 06:51:46 UTC
Body i have

Author Aaron Chia (741926884)
Sent 2017-12-05 06:51:45 UTC
Body you need sim cards

Author Aaron Chia (741926884)
Sent 2017-12-05 06:51:40 UTC
Body i have

Author Aaron Chia (741926884)
Sent 2017-12-05 06:51:36 UTC
Body look i need IDs

44. On August 8, 2018, AWS provided investigators with a copy of an internal investigation report relating to the fraudulent creation and use of Amazon retail and AWS cloud service accounts, including the MERRILL ACCOUNT. The AWS report identified

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

several accounts believed to be fraudulently created using Merrill's identity, which AWS identified as "Merrillot" (AWS) (the MERRILL ACCOUNT), "Merrillot2" (retail), "Corestratos" (retail), and "Mnmerrill" (retail). Through review of its records and open source information, AWS identified the suspect as "Matthew Ho (aka Ho Jun Jia, aka Jun Jia Ho)," who "appears to reside in Singapore and operates as a cryptocurrency vendor at times."

45. AWS also identified a second cryptocurrency vending site on which Ho appears to have been selling cryptocurrency. More specifically, according to the AWS report, "open source searches conducted on January 31, 2018, revealed the number [used to register the MERRILL ACCOUNT, namely, (714) 710-1077] was listed for the aliases 'Prefinity' (localbitcoins.com/accounts/profile/prefinity/) and 'Ethereum Vendor' (localethereum.com)."

46. The AWS report also provided a list of retail and AWS accounts registered to Ho, which included, among others, shorthand account identifiers "Project Quint" (AWS), "Prefinity" (retail), and "advent" (retail).[7] According to AWS, the phone number for the Ho accounts is listed as contact information for a cryptocurrency vendor, along with the phone number used to register the fraudulently obtained AWS MERRILL ACCOUNT using mnmerrill25@gmail.com (ACCOUNT #1).

47. Investigators observed that the identifier "advent" reappears in the username of **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**. Further, "Project Quint" is notably similar to ciel@projectquintessance.com (ACCOUNT #8), and "Prefinity" is, as discussed above, an alias used to sell cryptocurrency on localbitcoins.com and appears in other accounts attributed to Ho, such as matt@prefinity.com (ACCOUNT #3) and prefinity@outlook.jp (ACCOUNT #10), which is the alias of **advent@hotmail.co.jp (SUBJECT ACCOUNT #9)**.

[7] According to the AWS report, these identifiers were assigned by AWS in preparing the report. The basis is unknown to investigators.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

48. AWS further identified as part of its internal investigation an individual by the name of Aaron Chia as a possible accomplice of Matthew Ho. Notably, as noted above, Ho regularly communicated with Aaron Chia via Facebook, at times about cryptocurrency.

49. Based on my training and experience, and my involvement in this investigation, I believe that an individual known as "Matthew Ho" is the user of numerous accounts discussed in this affidavit, including **SUBJECT ACCOUNT #9**, and that the account records and information, including content, for **SUBJECT ACCOUNT #9** contain evidence of the user's true name and identity, location, participation in the criminal activity described herein, and possibly association and coordination with others. On about August 8, 2018, investigators submitted a preservation request to Microsoft regarding **SUBJECT ACCOUNT #9** as well as prefinity@outlook.jp (ACCOUNT #10).

BACKGROUND REGARDING MICROSOFT'S SERVICES

50. Microsoft is an internet service provider that offers a variety of online services including e-mail accounts (Outlook.com or Hotmail), cloud computing (Microsoft OneDrive and Office), gaming services (Xbox), video conferencing (Skype) and other services. A Microsoft account (formerly known as a Windows Live account) is what Microsoft customers may use to sign into Microsoft services such as Outlook.com (or Hotmail), Office, OneDrive, Skype, Xbox, Windows, and more. A user may create a Microsoft account with any e-mail address (Microsoft accounts are not limited to those who use Microsoft e-mail accounts) and a password and thereafter use that e-mail address and password to sign in to any Microsoft program or service.

51. In my training and experience E-mail providers like Microsoft typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via a website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account, which can help establish the individual or individuals who had dominion and control over the account

52. In general, an e-mail that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Microsoft's servers for a certain period of time.

53. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination. Microsoft often maintains a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from Microsoft's server, the e-mail can remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue to be available on Microsoft's servers for a certain period of time.

54. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Microsoft but may not include all of these categories of data.

55. Microsoft provides a variety of online, or "cloud," services in addition to email access, to the public and to customers who utilize hotmail accounts that are served by Microsoft. Microsoft's various cloud services are associated with a single Microsoft account, which is typically associated with a Microsoft email address, but can be associated with any email address. The various cloud services provided by Microsoft are optional, and can be turned "on" or "off" by the user.

56. In providing services such as Outlook, OneDrive, Xbox, calendar services, online file storage, storage of browsing history, storage of search history, and locations

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

history, Microsoft collects information that constitute evidence of the crimes under investigation. For example, such evidence can be used to discover or confirm the identity and location users of the service at a particular time.

57. Microsoft is also able to provide information that will assist law enforcement in identifying other accounts associated with the SUBJECT ACCOUNT. In particular, Microsoft can provide information identifying and relating to other accounts used by the same subscriber. This information includes any forwarding or fetching accounts[8] related to the SUBJECT ACCOUNT; all other Microsoft accounts linked to the SUBJECT ACCOUNT because they were accessed from the same computer (referred to as "cookie overlap"); all other Microsoft accounts that list the same SMS phone number[9] as the SUBJECT ACCOUNT; all other Microsoft accounts that list the same recovery email addresses as the SUBJECT ACCOUNT; and all other Microsoft accounts that share the same creation IP addresses[10] as the SUBJECT ACCOUNT. This information will assist law information in determine who controls the SUBJECT ACCOUNT and in identifying other accounts utilized by the malware scheme.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

58. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit Microsoft, and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to Microsoft with direction that it identify the Microsoft account described in Attachment A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section I of Attachment B to this affidavit.

---

[8] A forwarding or fetching account related to one of subject accounts would be a separate email account that can be setup by the user to receive copies of all of the email sent to the subject account.
[9] The SMS phone number of a Microsoft account is used by Microsoft as an additional security precaution to verify the identity of the user by sending a text message with a code that must be entered in addition to the password to log into the account. This ensures that only a person with both the password and the phone tied to the SMS phone number can make changes to the account.
[10] The creation IP address is the IP address from which the Microsoft account was created.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

59. The search warrant will direct Microsoft to create an exact copy of the specified account and records, including an exact copy of the contents of the hard disk drive or drives installed on the server associated with **SUBJECT ACCOUNT #9**, or the original drives.

60. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

61. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

CONCLUSION

62. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

REQUEST FOR SEALING

63. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the target(s) of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Joel Martini, Affiant
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 15th day of August, 2018.

HONORABLE JAMES P. DONOHUE
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Account to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following account:

advent@hotmail.co.jp ("**SUBJECT ACCOUNT**")

as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by Microsoft Corporation ("Microsoft"), an e-mail and service provider headquartered in Redmond, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Items to be Seized

I. Section I - Information to be disclosed by Microsoft, for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Microsoft, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account January 1, 2017 to the present, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. all GPS, Wi-Fi, or cell tower proximity records related to the account and/or account contents;

f. any Microsoft Groups information and/or records including member lists, e-mail addresses of members, messages, files, calendars, database content, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

photographs;

g. any Microsoft Chat/Messenger information and/or records, including any Microsoft Chat/Messenger Friends list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on Microsoft servers;

h. any Flickr content including Flickr e-mail, photographs and user comments, IP address and timestamp of content uploaded to account;

i. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

This Search Warrant also requires Microsoft to produce the following information for accounts associated with any of the Target Accounts (collectively the "Linked Subject Accounts"):

a. a list of all other accounts linked to the SUBJECT ACCOUNT because of cookie overlap with any SUBJECT ACCOUNT;

b. a list of all other accounts that list the same SMS phone number as any of the SUBJECT ACCOUNT;

c. a list of all other accounts that list the same recovery email address as any of the SUBJECT ACCOUNT;

d. a list of all other accounts that shared the same creation IP address as any of the SUBJECT ACCOUNT within 30 days of creation;

e. Subscriber records for each of the Linked Subject Accounts including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Microsoft in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts.

NOTE: The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18 United States Code, Sections 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(4) (Computer Fraud); 1343 (Wire Fraud); and 1956 (Money Laundering), those violations occurring between approximately October 2017 and the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Content that serves to identify any person who uses or accesses the account or who exercises in any way any dominion or control over the account;

b. Content relating to or referring to the name "Merrill";

c. Content relating to or referring to "Riot Games";

d. Content relating to the creation or use of mnmerrill25@gmail.com;

e. Content relating to the creation of an account at an email or cloud services provider, including Google, Amazon, or Amazon Web Services;

f. Content relating to the data usage of cloud services account;

g. Content relating to acquisition, mining, purchase, sale, or transfer of cryptocurrency, such as Bitcoin and Ethereum, including use of or access to cryptocurrency wallets or mining-related material;

h. Content referencing or relating to cryptocurrency vending websites, such as localbitcoins.com and localethereum.com;

i. Content relating to use of monikers "Prefinity" or "Ethereum Vendor";

j. Content relating to the creation or maintenance of domain

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

"prefinity.com";

k. Content relating to cloud computing services and the acquisition, maintenance, or use of related accounts;

l. Content relating to communications with Amazon, Amazon Web Services, or Google Cloud Services;

m. Content that identifies victims of identity theft perpetrated by the account holder or his/her associates;

n. Content that constitute communications in furtherance of the crimes enumerated above;

o. Content that may identify assets including bank accounts, commodities accounts, trading accounts, cryptocurrency wallets, personal property and/or real estate that may represent proceeds of computer intrusion activity or fraud or are traceable to such proceeds;

p. Content that may reveal the current or past location of the individual or individuals using the account;

q. Content that may reveal the identities of and relationships between co-conspirators;

r. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over the specified account as well as records or information that may reveal the true identities of these individuals;

s. Other log records, including IP address captures, associated with the specified account;

t. Subscriber records associated with the specified account, including 1) names, e-mail addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

addresses, or any other unique device identifiers recorded by Microsoft in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

u. Records of communications between Microsoft and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

v. Android identification number, MEID, and cellular telephone number Information identifying accounts that are linked or associated with the account.

w. Android identification number, MEID, and cellular telephone number Information identifying accounts that are linked or associated with the account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Microsoft Corporation (Microsoft), and my official title is _____. I am a custodian of records for Microsoft. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Microsoft and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Microsoft; and

c. such records were made by Microsoft as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date: _____

_____
Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970